Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Conveyant Systems Sentry E9-1-1 Solution with Avaya IP Office 9.1 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the Conveyant Systems E9-1-1 Solution with Avaya IP Office. The Conveyant Systems Sentry E9-1-1 Solution provides on-site notification when an emergency call has been placed.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required to integrate the Conveyant Systems E9-1-1 Solution (hereafter, also referred to as "Sentry") with Avaya IP Office. Sentry provides on-site notification when an emergency call has been placed. Sentry is a software based solution that utilized the following components for compliance testing: the Sentinel web server, Sentry database, Sentry SNMP Listener, and the Beacon Alert Agent.

2. General Test Approach and Test Results

This section includes the general test approach, what was covered, and results of the testing.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The general test approach was to verify the integration of Sentry with Avaya IP Office. Various emergency calls were placed from Avaya IP Office telephones to verify SNMP traps were properly logged and displayed (via a pop-up alerts) by Sentry. Sentry's email notification of the alert was not tested.

Additionally, basic serviceability testing examined the handling of and recovery from error conditions (such as network disconnects and power failures).

2.2. Test Results

The Conveyant Systems Sentry E9-1-1 Solution successfully passed compliance testing with the following observation:

- The Windows 2008 R2 Enterprise Server used to host the Conveyant Systems Sentry E9-1-1 solution was not consistently starting the "Sentry Licensing Service" on its first attempt. As a workaround to this Windows issue, the Recovery tab within the Properties of the service was configured to "Restart the Service" upon failure. Note, Administrators should verify and ensure all Conveyant System services are starting automatically.

2.3. Support

For technical support with the Conveyant Systems Sentry E9-1-1 solution, contact Conveyant Systems at:

- **Web**: http://www.conveyant.com/
- **Email**: support@conveyant.com
- **Phone**: (949) 756-7171

3. Reference Configuration

Figure 1 below illustrates the configuration used to compliance test the Conveyant Systems Sentry E9-1-1 solution with Avaya IP Office. The Conveyant Systems Sentry E9-1-1 Solution (utilizing the Sentinel web server, Sentry database, Sentry SNMP Listener, and the Beacon Alert Agent) was installed on a Windows Server 2008 R2 Enterprise server.

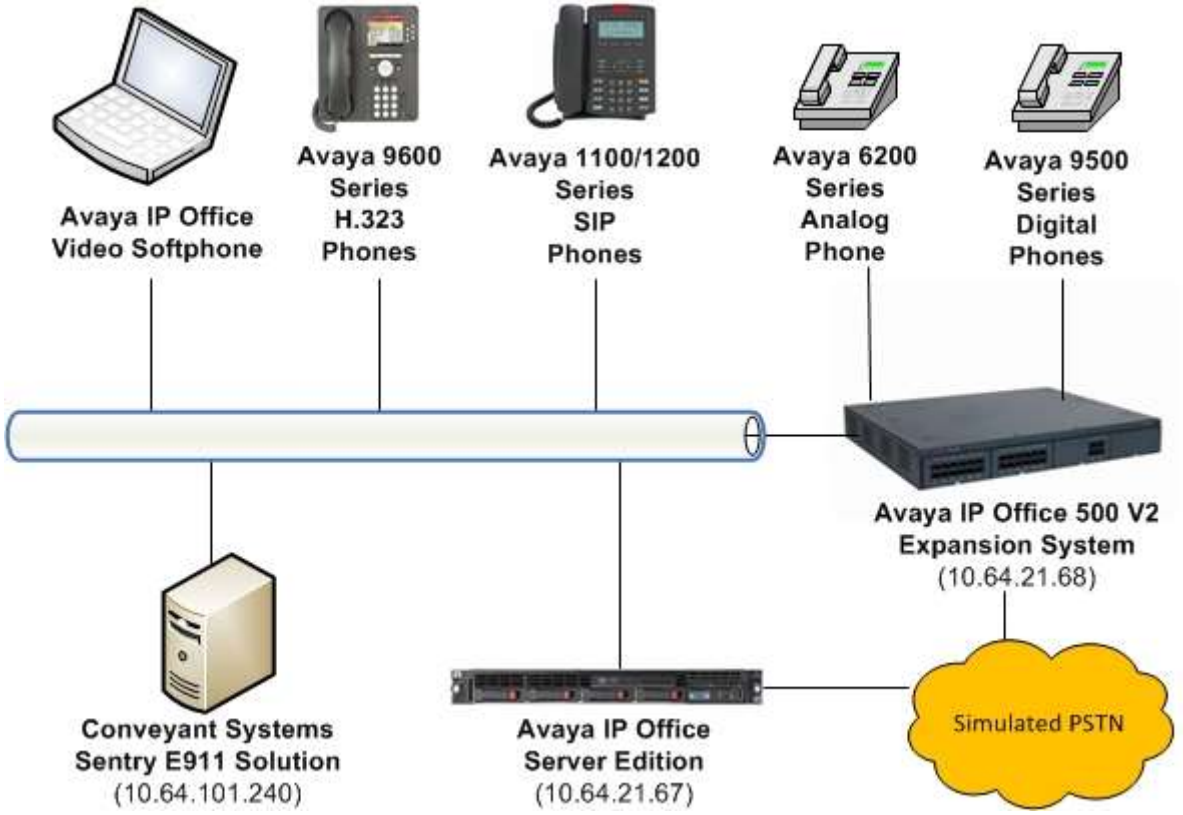


Figure 1: Conveyant Systems Sentry E9-1-1 Solution with Avaya IP Office

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

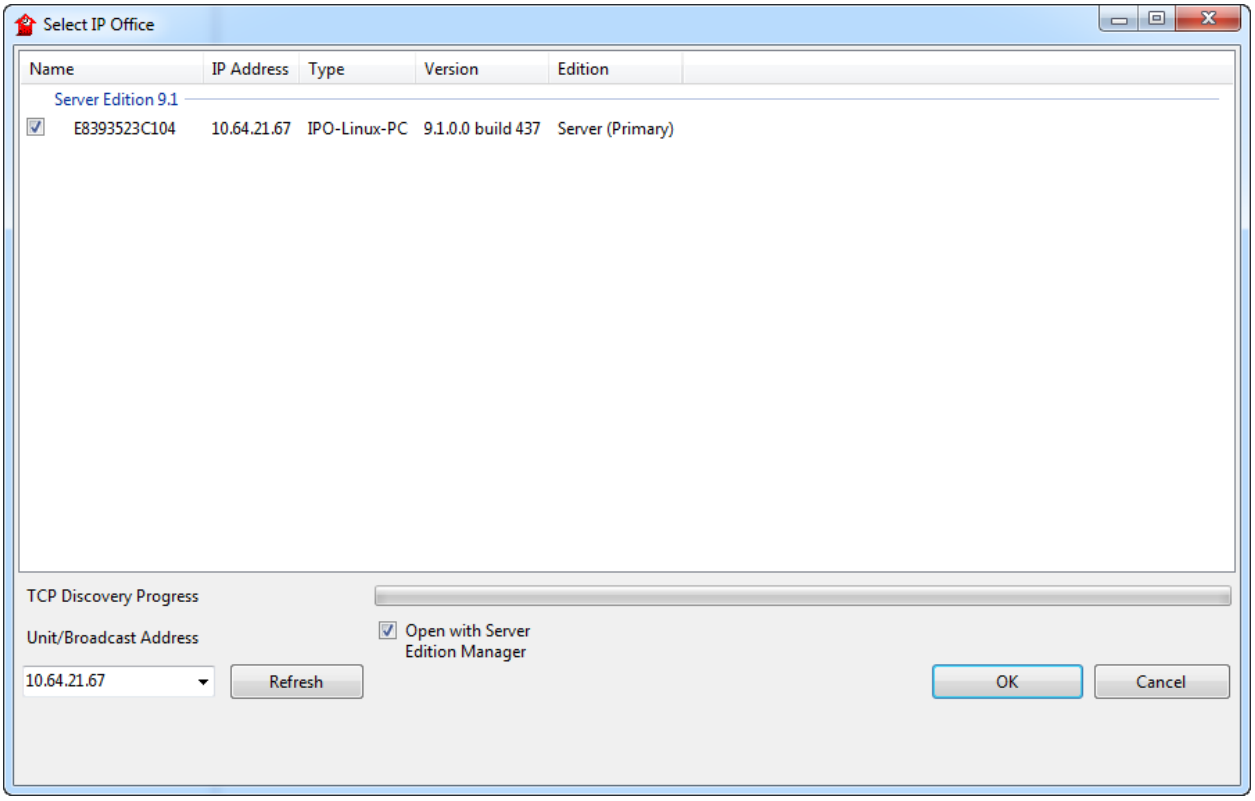
Equipment/Software	Release/Version
Avaya IP Office Server Edition server (Linux)	9.1.0.0 Build 437
Avaya IP Office 500 V2 Expansion Module	9.1.0.0 Build 437
Avaya 1100/1200 Series IP Deskphones	SIP 4.4
Avaya 9600 Series IP Deskphones	H.323 6.4
Avaya IP Office Softphone	3.2.3.49
Avaya 9500 Series Digital Phone	-
Avaya 6200 Series Analog Phone	-
Conveyant Systems Sentry E9-1-1 Solution server (Windows 2008 R2 Enterprise)	1.7.1010

Note: ***Testing was performed with IP Office Server Edition and an Expansion IP Office 500 V2. Testing also applies to an IP Office 500 V2 standalone system, and all IP Office Server Edition configurations.***

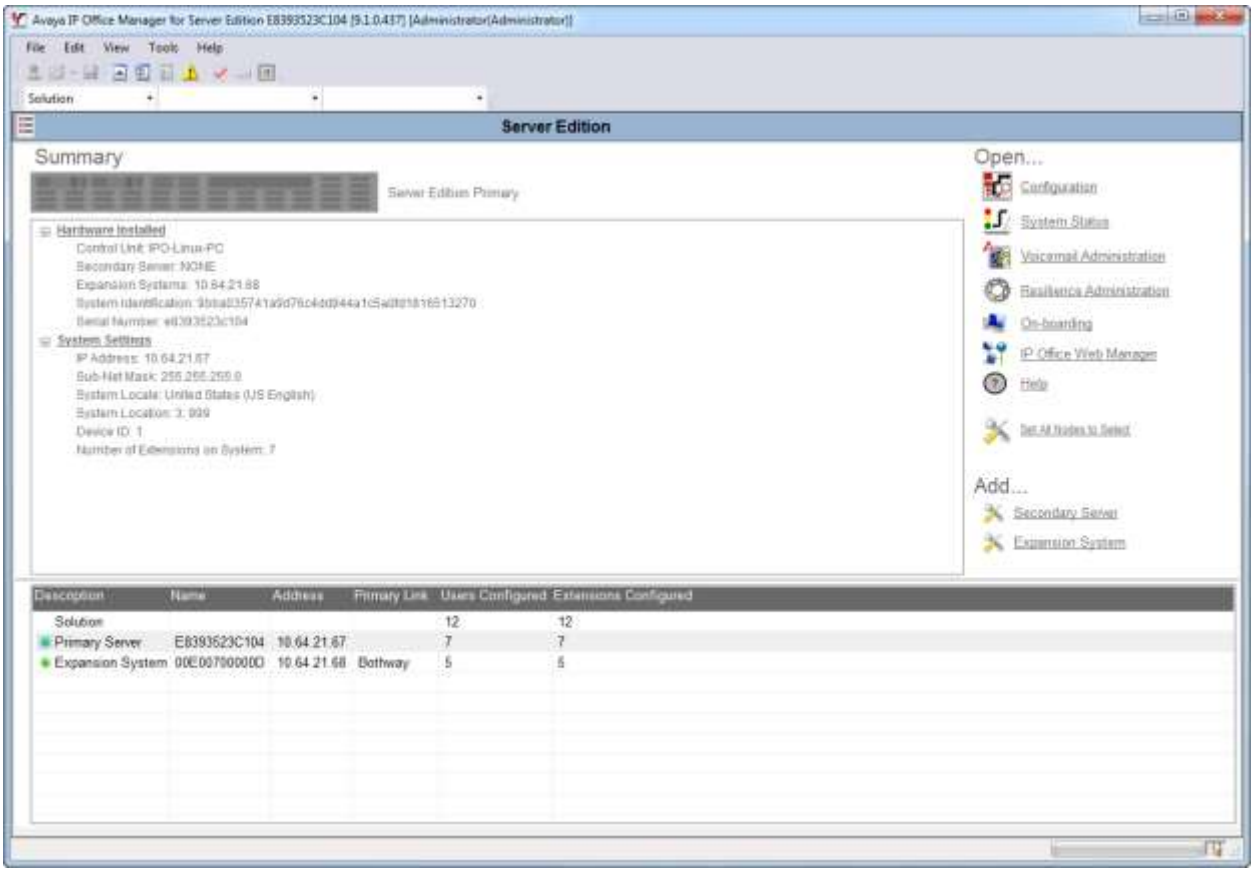
5. Configure Avaya IP Office

This section describes the Avaya IP Office Server Edition configuration necessary to support integration with the Conveyant Systems Sentry E9-1-1 solution. It is assumed that the initial installation and provisioning of the Server Edition Primary Server and Expansion System has been previously completed and therefore is not covered in these Application Notes. For information on these installation tasks, refer to reference **[1]** in the **Additional References** section.

The solution is configured through the Avaya IP Office Server Edition Manager PC application. From the PC running the IP Office Manager application, select **Start → All Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, and select the proper Avaya IP Office Server Edition system. Log in using appropriate credentials.



The Solution View screen will appear, similar to the one shown below. This screen includes the system inventory of the servers and links for administration and configuration tasks.



In the screens presented in these sub-sections, the View menu was configured to show the Navigation pane on the left side, the Group pane in the center and the Details pane on the right side. These panes will be referenced throughout the rest of this section.

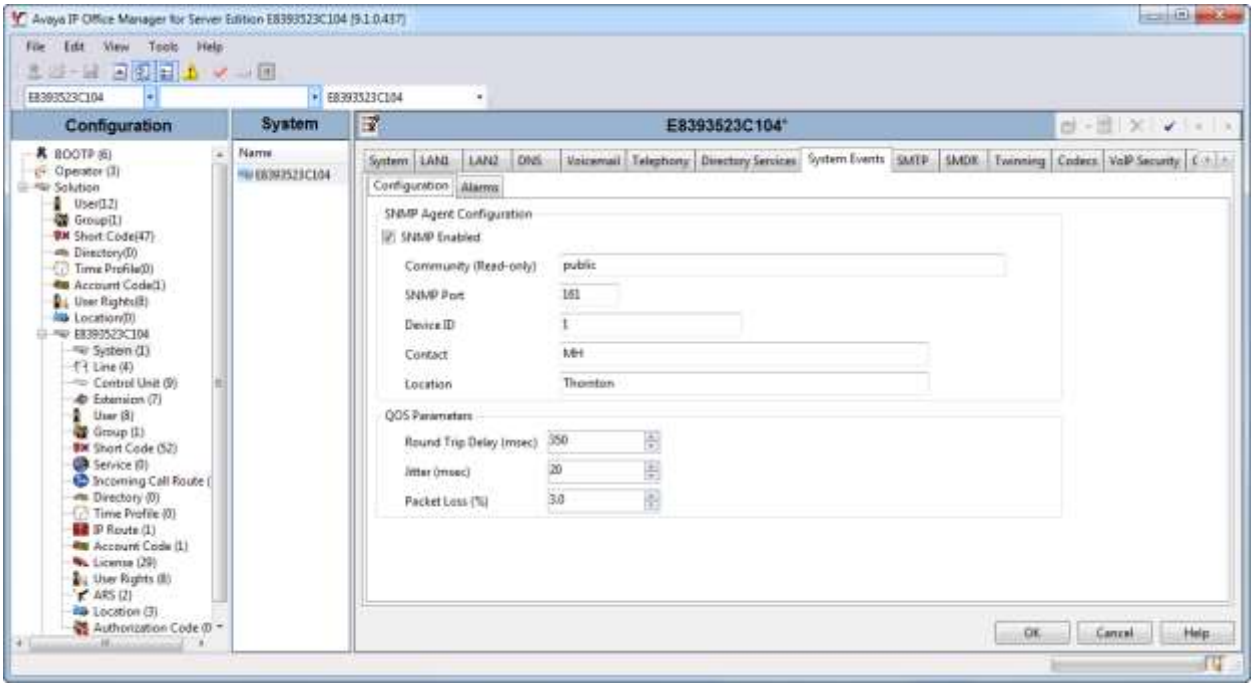
Note that the Navigation pane includes solution settings, under the Solution menu, which apply to all the systems in the Server Edition solution, and individual system settings, each grouped under the Primary Server and the Expansion System menus.

For each form where modifications have been made, the user must click the **OK** button to submit the changes. After all changes have been made to the system, click **File → Save Configuration**.

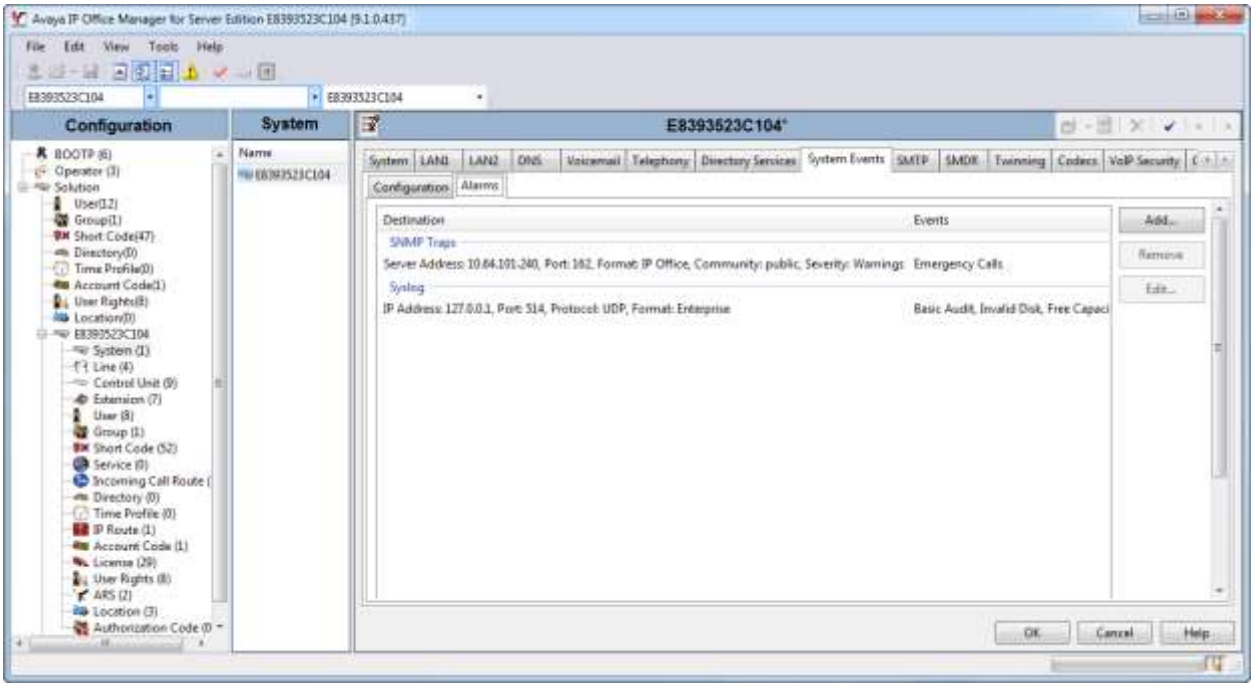
Note, the sub-sections below show the steps required to configure SNMP traps and emergency calls for Primary server only. The same steps MUST be performed for each Secondary Server and Expansion System within a solution using the appropriate values for each server/expansion system.

5.1. Configure SNMP Traps for Emergency Calls

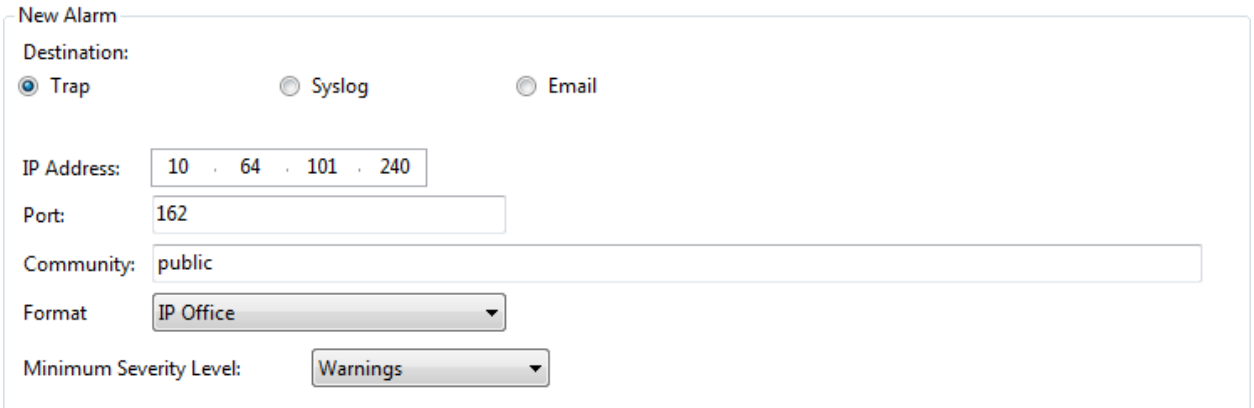
To configure SNMP traps for Emergency calls on the Primary Server, complete the following steps. Navigate to the Primary system, in this case, **E8393523C104 → System (1)** in the Navigation pane and then select the **System Events** tab in the Details pane. Under the **Configuration** sub-tab, check the box for **SNMP Enabled**. Fill in the remaining fields with values appropriate for the site. The screen below shows the values used during compliance testing.



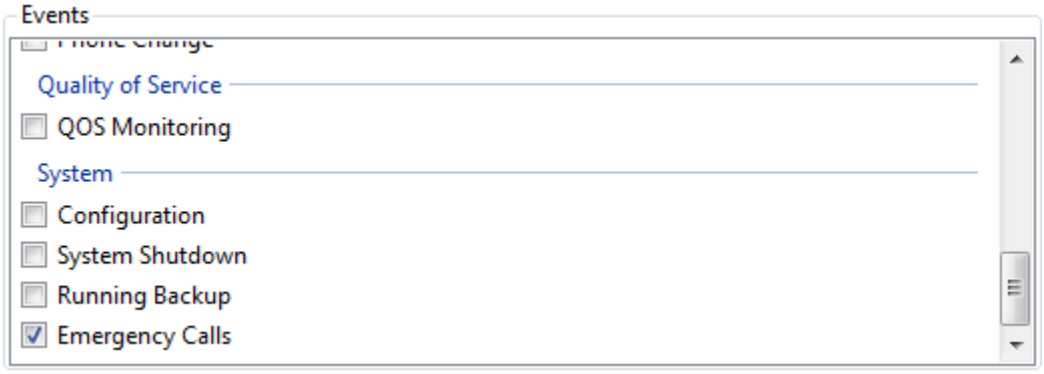
Click the **Alarms** sub-tab, and click the **Add...** button or the right side of the Details pane.



In the **New Alarm** section, select the **Trap** radio button. For **IP Address**, enter the IP Address of the Conveyant Systems Sentry E9-1-1 Solution server. This is the IP address of the SNMP server to which trap information is sent. Enter the SNMP transmit **Port** (default = 162). The SNMP **Community** value entered for the transmitted traps must be matched by the receiving SNMP server. Select *IP Office* for **Format**. The **Minimum Security Level** can be left at the default level of *Warnings*.



In the **Events** section, scroll to the bottom and check **Emergency Calls**.



The alarms configured above trigger when Avaya IP Office determines that an emergency call has been dialed and the call has been routed, regardless of whether the call is successful. For example, if an emergency call is dialed, but all lines/trunks are down, an SNMP trap will still be generated when Avaya IP Office attempts to route the emergency call. The trap will contain all the same information whether or not the emergency call is actually successful.

5.2. Configure Emergency Calls

IP Office Manager expects that the configuration of each system to contain at least one short code that is set to use the Dial Emergency feature. If no such short code is present in the configuration, then Manager will display an error warning. The importance of the Dial Emergency feature is that it overrides all external call barring that may have been applied to the user whose dialing has been matched to the short code. You must still ensure that no other short code or extension match occurs that would prevent the dialing of an emergency number being matched to the short code.

The short code (or codes) can be added as a system short code or as an ARS record short code. If the Dial Emergency short code is added at the solution level, that short code is automatically replicated into the configuration of all servers in the network and must be suitable for dialing by users on all systems. Separate Dial Emergency short codes can be added to the configuration of an individual system. Those short codes will only be useable by users currently hosted on the system including users who have hot-desked onto an extension supported by the system. For compliance testing, short codes were configured for the individual systems.

It is the installer's/administrator's responsibility to ensure that a Dial Emergency short code or codes are useable by all users. It is also their responsibility to ensure that either:

- The trunks via which the resulting call may be routed are matched to the physical location to which emergency service will be dispatched.

  or

- The outgoing calling line ID number sent with the call matches the physical location from which the user is dialing.

When configuring locations, consult local guidelines. For example, regions may require identification based on building or building floor. Floors may be subdivided based on number of staff or the location of hazardous materials. Typically, fire alarm planning will have defined zones based on these or similar requirements.

Routing of emergency calls is based on a call resolving to a Dial Emergency short code. Based on the location value for the extension making the call, routing is performed as configured in the Emergency ARS.

To configure and test emergency call routing within Avaya IP Office perform the following steps:

1. Create a Dial Emergency short code.

Note that the Line Group ID value in the Dial Emergency short code is the fallback route. If the system cannot find a location or an Emergency ARS, it will try to use the Line Group ID to route the call.

2. Create an ARS containing a Dial Emergency short code.

3. Create a Location and set the Emergency ARS to the ARS created in step 2.

4. Open the Extn tab for an extension that will use the location defined in step 3 and set the Location value to the location defined in step 3.

   Note that once you define a location, you must set a system Location value on the **System → System** page.

   For non-IP based extensions, the system location value is used as the default. For IP based extensions, the location value is set to Automatic. An attempt is made to match the extension's IP address to the subnet configured in the location. If the match cannot be made, the location value defaults to the system location value.

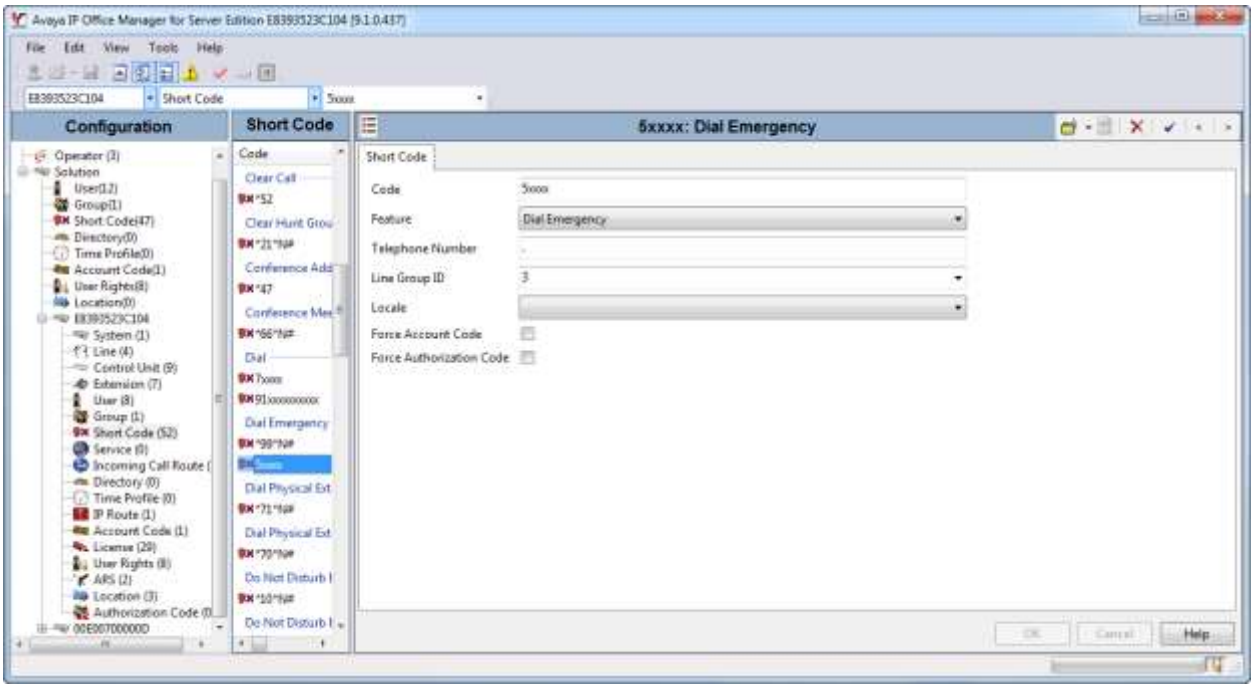
5. To test an emergency call, from the extension used in step 3, dial the Dial Emergency short code. Avaya IP Office checks the location value and determines the emergency ARS set for the location. Once the emergency ARS is found, Avaya IP Office will try to match the Telephone Number in the Dial Emergency short code to a short code in the ARS and use it to make the emergency call.

The sections below show the configuration used during compliance testing.

5.3. Short Code

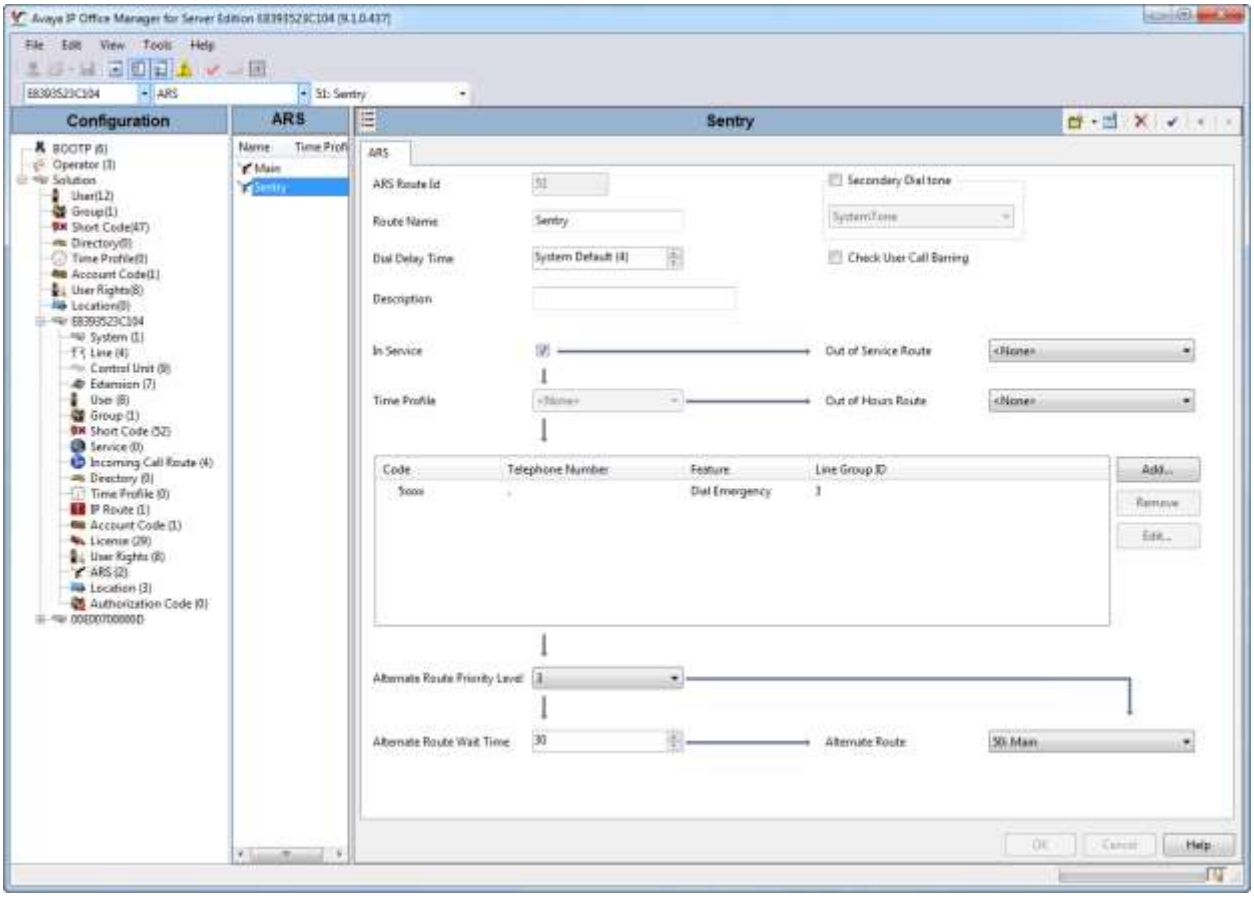
On the left Navigation pane, right-click **Short Code** for the Primary Server and select **New** (not shown). The screen below shows short code 5xxxx was created. For compliance testing, calls to 50000 through 59999 were used to test emergency calls rather than placing actual 911 calls. Set the **Feature** to *Dial Emergency*. The **Telephone Number** was set to "." to leave the dialed number unaltered.

Note that the **Line Group ID** value in the Dial Emergency short code here is the fallback route. If the system cannot find a location or an Emergency ARS, it will try to use the **Line Group ID** to route the call.

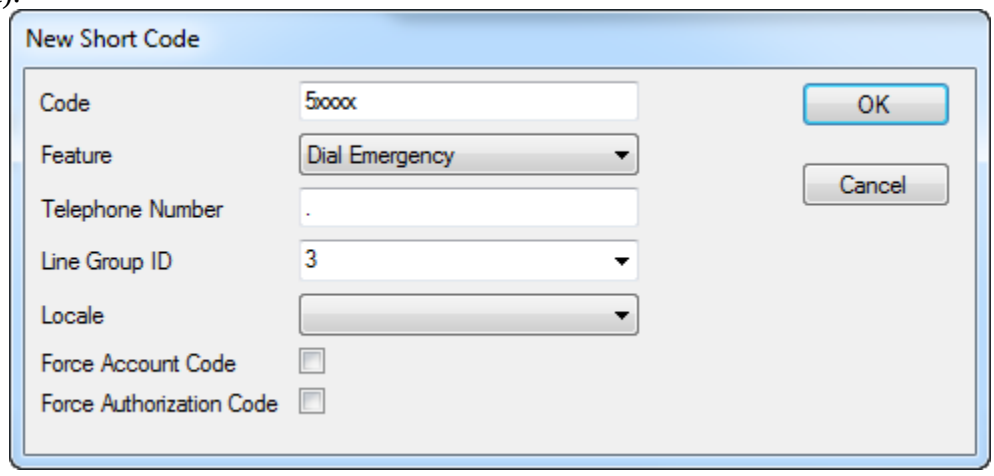


5.4. ARS

On the left Navigation pane, right-click **ARS** for the Primary Server and select **New** (not shown). Provide a descriptive **Route Name** and ensure **In Service** is checked. Click the **Add…** button on the right to add an ARS short code.

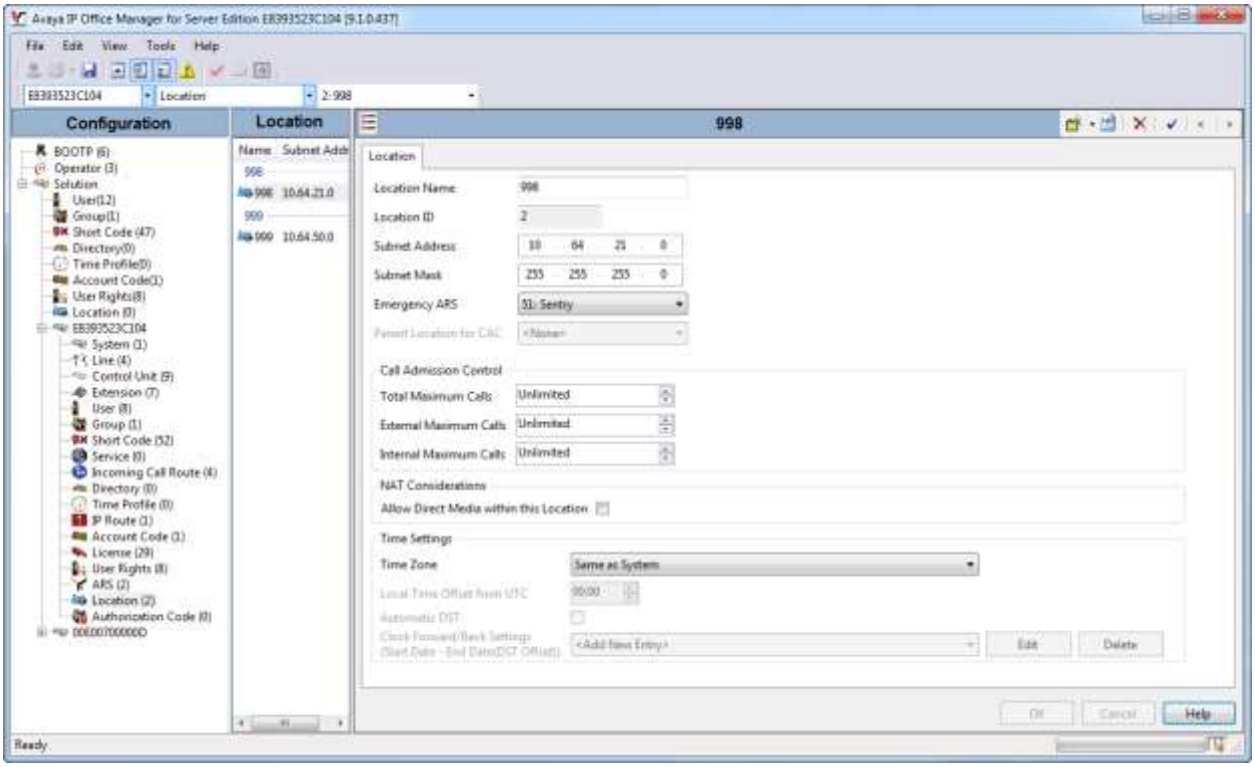


The screen below shows short code 5xxxx was created. For compliance testing, calls to 50000 through 59999 were used to test emergency calls rather than placing actual 911 calls. Set the **Feature** to *Dial Emergency*. The **Telephone Number** was set to "." to leave the dialed number unaltered. Set the **Line Group ID** value to the line to be used to route emergency calls (configuration of lines/trunks are assumed to already be in place and is outside the scope of this document).



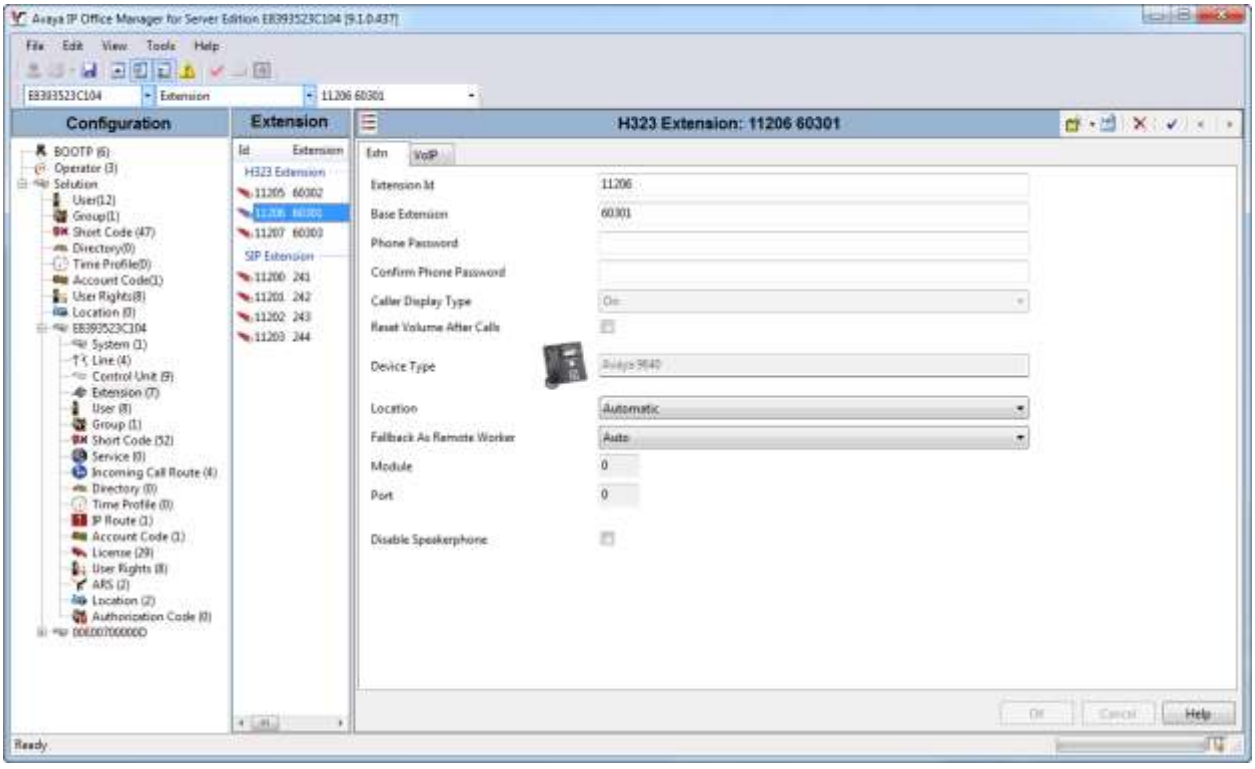
5.5. Locations

On the left Navigation pane, right-click **Location** for the Primary Server and select **New** (not shown). Enter a numeric **Location Name**. Note, **Location Name** field accepts characters; however, this field will be used to match the ERL/ELE value configured for a Location on Sentry (see **Section 6.2**), and the ERL/ELE value must be numeric. Use the **Subnet Address** and **Subnet mask** fields to define the IP addresses associated with this Location. The subnet where these IP addresses reside must be unique across all configured Locations. Set **Emergency ARS** to the ARS entry created in **Section 5.4**.



5.6. Extensions

Associate each extension with a Location. On the left Navigation pane, click **Extension** for the Primary Server and then select a desired extension to configure from the middle Group pane. In the Details Pane on the right, set the **Location** for the extension. The **Location** can be set to *Automatic* or to a specific Location that was configured in the previous section.



6. Configure Conveyant Systems Sentry E9-1-1 Solution

It is assumed that the Sentry server has been installed, configured, and is ready for the integration with Avaya IP Office. The Sentry Software Users Guide can be obtained by contacting Conveyant Systems. The sub-sections below only provide the steps required to configure the Conveyant Systems Sentry E9-1-1 Solution to interoperate with Avaya IP Office.

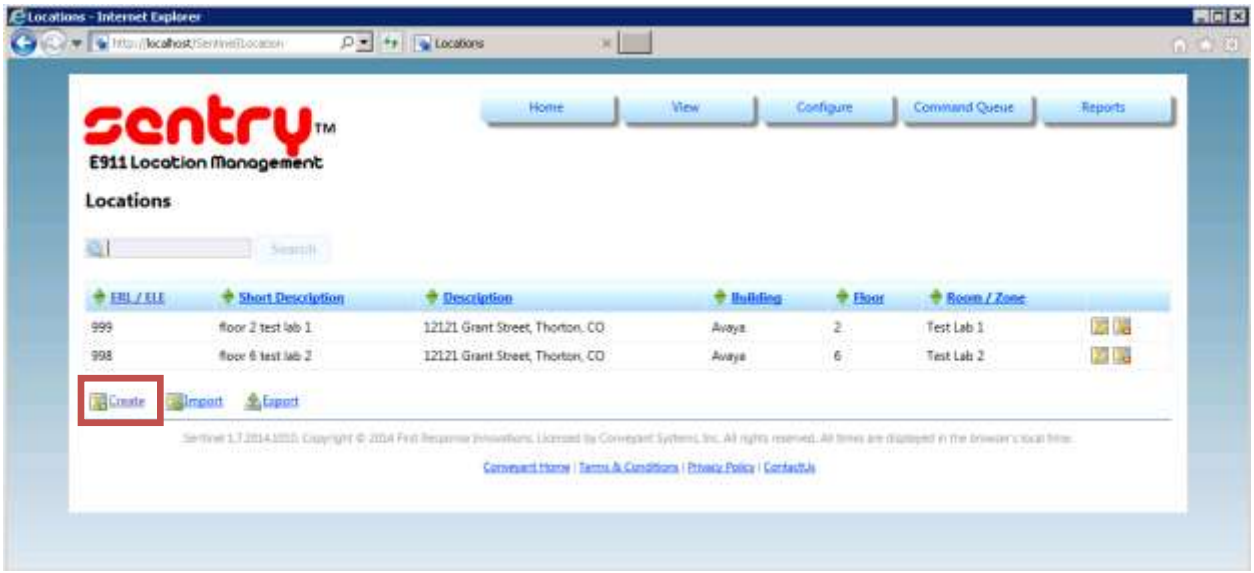
6.1. Sentinel Web Interface

Access the Sentinel web interface by opening a web browser and entering the following URL: ***http://localhost/Sentinel***.

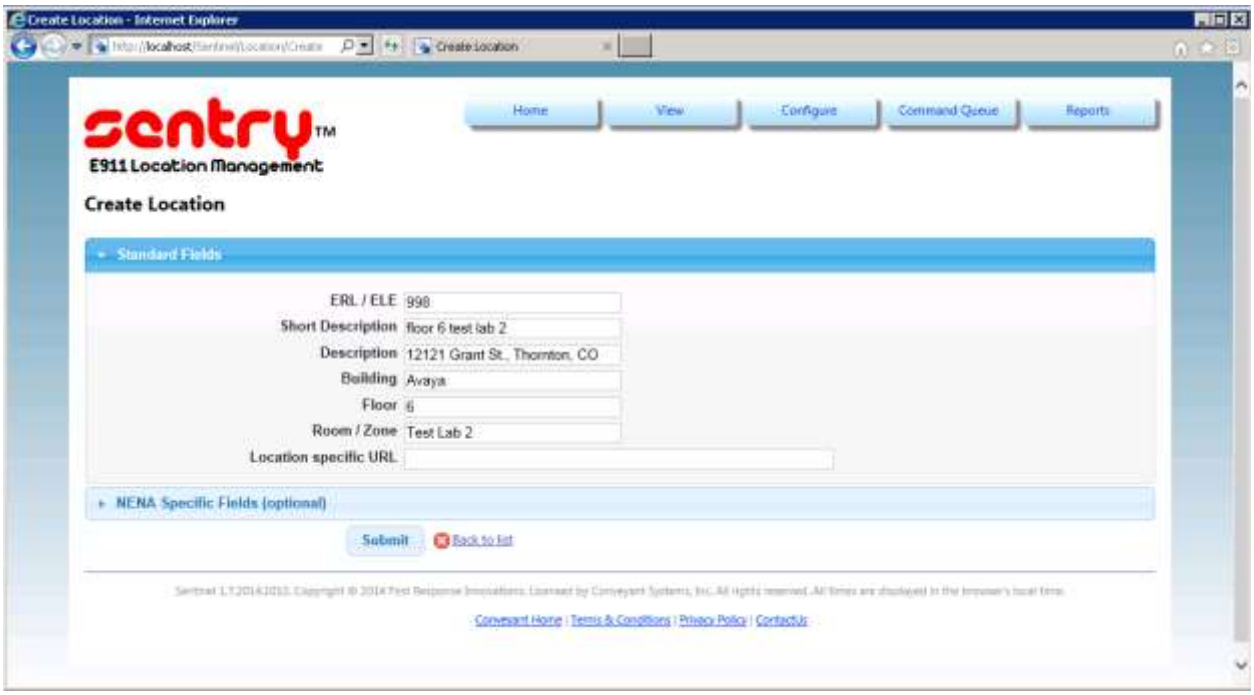
6.2. Configure Locations

Under **Configure** from the top menu bar, click **Locations**.

Click **Create** to add a new Location.



For each Location, set the **ERL/ELE** field to match the appropriate **Location Name** defined in **Section 5.5**. Fill in the remaining fields for the Location and click **Submit**.

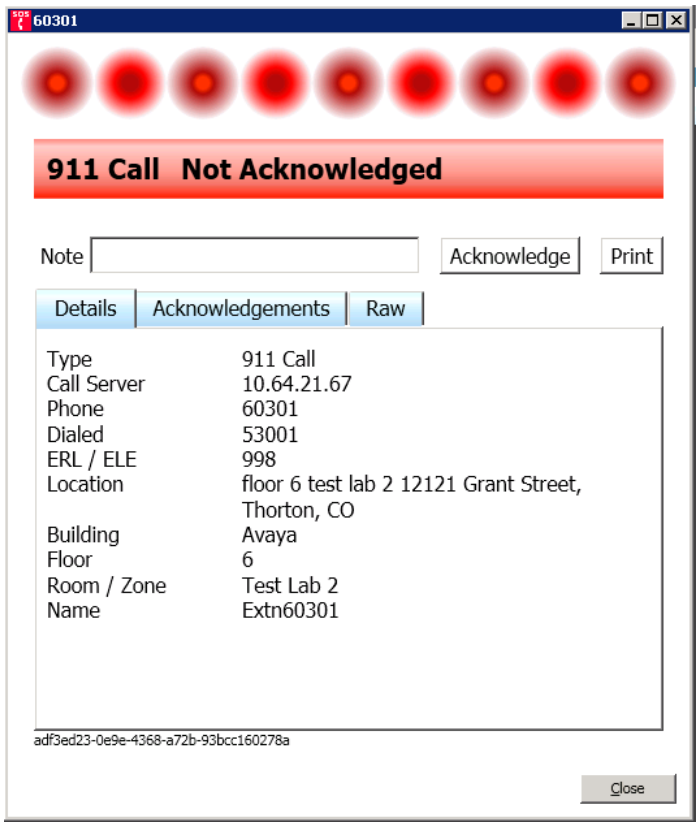


7. Verification Steps

This section includes some steps that can be followed to verify the configuration.

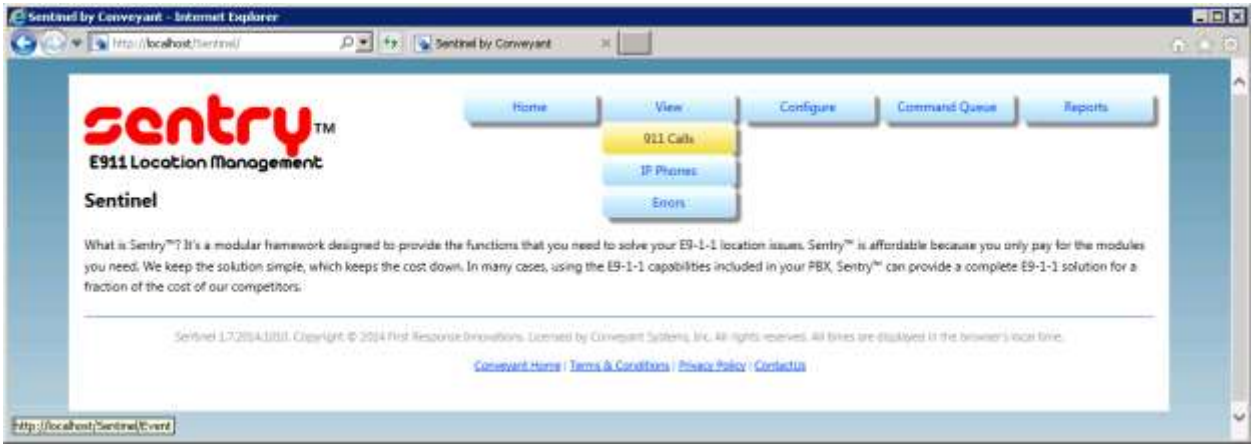
7.1. Verify On-site Notification and Emergency Call Log

Place an emergency call. Verify the Sentry Beacon pops an Alert window such as the one shown below. Verify the data in each of the tabs.



7.2. Verify Emergency Call Messages

Open the Sentinel web interface (refer **to Section 6.1**). Under **View** from the top menu bar, click **911 Calls**.



Verify each emergency call appears in the messages list with the proper data.

8. Conclusion

The Conveyant Systems Sentry E9-1-1 Solution passed compliance testing. These Application Notes describe the procedures required for the Conveyant Systems Sentry E9-1-1 Solution to interoperate with Avaya IPO Office to support the reference configuration shown in **Figure 1**. Refer to **Section 2.2** for testing result details and any observations noted during testing.

9. Additional References

Product documentation for Avaya products may be found at: http://support.avaya.com.

[1] *IP Office Manager*, Document ID 15-601011, Issue 9.0.4, December 2014.

Product information for the Conveyant Systems Sentry E9-1-1 Solution may be obtained by contacting Conveyant Systems.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.